FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/FDIS
14950

ISO/TC **20**/SC **14**

Secretariat: **ANSI**

Voting begins on:
2003-10-30

Voting terminates on:
2003-12-30

Space systems — Unmanned spacecraft operability

Systèmes spatiaux — Opérabilité des satellites non habités

Please see the administrative notes on page iii

Reference number
ISO/FDIS 14950:2003(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

In accordance with the provisions of Council Resolution 15/1993, this document is **circulated in the English language only**.

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 14950 was prepared by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*.

The key objectives of this International Standard are:

- to ensure that a spacecraft operates in a safe and cost-effective manner and may be operated with an optimized workload;
- to facilitate and/or enhance the tasks of preparation for, execution and evaluation of, spacecraft check-out and mission operations activities;
- to facilitate the tasks of spacecraft prime contractors when preparing a proposal in answer to an international request for proposal (RFP).

This International Standard is written in such a way that technological advances will not invalidate the International Standard. Thus, this International Standard is not project or machine specific.

The operation of the space segment to meet mission-specific requirements is outside the scope of this International Standard.

0.3 Conventions

Requirements are identified by an acronym, which indicates the nature/grouping of the requirement, followed by a serial number, and appear in bold type (e.g. **OBSERV-0010)**. The serial number comprises four digits starting at 0010 and is incremented by 10 to facilitate configuration control for later versions of the document. Where a major requirement is broken down into subsidiary requirements, the serial number is extended to reflect this structure (e.g. **TEST-1010.1** would represent the first sub-requirement of requirement 1 relating to testability). General operability requirements are numbered in the range 0010 to 0999, while detailed operability requirements are numbered in the range 1010 to 1999.

Some of the detailed operability requirements in Clause 6 are only relevant for a given level of on-board autonomy. In such cases, the corresponding autonomy level (as defined in Clause 4), is indicated as a super-script following the requirement ID. For example, **FAULT-1100**$^{\mathbf{C3}}$.

Some requirements introduce quantities for which values cannot be defined across the board but will need to be defined on a mission-by-mission basis (e.g. time intervals, response times, etc.). These are termed mission constants and are identified within this International Standard in “<>” (for example, <TC_VERIF_DELAY>) and, where appropriate, typical values may be indicated. These mission constants are also summarised, for information only, in Annexlnex

Space systems — Unmanned spacecraft operability

1 Scope

This International Standard defines the essential properties pertaining to the operation of unmanned spacecraft and defines requirements and guidelines for spacecraft on-board functions in order to enable a specified ground segment to operate the spacecraft in any nominal or predefined contingency situation.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced as well as the capacity to optimize mission products according to the mission events

3.1.5
observability
ability to acquire operationally significant information for physical and logical parameters on-board the spacecraft

NOTE 1 This information is delivered to the ground through the telemetry channel and/or made available to on-board processors.

NOTE 2 The definition of observable parameters is a key requirement for operating spacecraft, monitoring the behaviour of all on-board systems, performing diagnosis of anomalies, and collecting sufficient information for feedback into ground-based models.

3.1.6
operation
⟨spacecraft⟩

3.2.2
autonomy
extent to which a spacecraft can handle nominal and/or contingency operations without ground intervention

3.2.3
chain
set of hardware and/or software units that operate together to achieve a given function

EXAMPLE An attitude and orbit-control-subsystem (AOCS) processor and its software and a set of AOCS sensors and actuators together constitute an AOCS chain.

3.2.4
control loop
mechanisms to maintain a parameter or a set of parameters within prescribed limits

NOTE A control loop normally consists of a set of measurements and responses (commands) related according to a function, algorithm, or set of rules.

3.2.5
device telecommand
telecommand that is routed to and executed by on-board hardware

EXAMPLE A relay switching telecommand or a telecommand to load an on-board register.

3.2.6
ground segment
all ground facilities and personnel involved in the preparation and/or execution of mission operations

3.2.7
high level telemetry
telemetry processed from the low level telemetry by an on-board application process

3.2.8
low level telemetry
elementary readable on-board information

EXAMPLE Register readout or relay status.

3.2.9
memory
any on-board memory area, whether main memory or storage memory, such as disk, tape, or bubble-memory

3.2.10
mission management
on-board functionality that allows a mission to undertake routine operations highly autonomously with the minimum of ground intervention

3.2.11
mission manager

3.2.12
no ground contact

period of time during a mission when ground contact is not possible due to the unavailability of the telecommand/telemetry links

NOTE The reasons for this unavailability can include:

a) predictable events such as:

   1) non-permanent visibility due to spacecraft orbit characteristics combined with radio frequency coverage of telemetry and telecommand links;

   2) time-shared access to the spacecraft;

b) unpredictable events such as:

   1) spacecraft attitude depointing;

   2) on-board failure of the telemetry and telecommand links;

   3) ground station failure/unavailability;

   4) link budget degradation.

3.2.13
on-board fault management

on-board functionality that allows the detection and management of on-board failures without ground intervention

NOTE 1 The primary objective of on-board fault management is to ensure the survival of the spacecraft.

NOTE 2 Where possible without hazard to the spacecraft, and within the mission constraints, on-board fault management shall maintain payload operations.

NOTE 3 In addition, on-board fault management should assist in rapid diagnosis and subsequent reconfiguration back to an optimal operational status.

3.2.14
on-board monitoring

set of processing functions that is applied to a set of on-board parameters

NOTE 1 These functions can include limit/status/delta checking, the evaluation of statistics, including minimum and maximum values over a time interval, etc.

NOTE 2 Detected events or evaluation results are telemetred to ground.

NOTE 3 The scope of the function can be even wider, e.g. to include the triggering of on-board actions in response to detected events.

3.2.15
on-board operations scheduling

capability for controlling and executing commands that were loaded in advance from the ground

NOTE In its simplest form, the on-board operations schedule stores time-tagged commands loaded from the ground and releases them to the destination application process when their on-board time is reached, but with no feedback being generated by the destination application process.

3.2.16
on-board operations procedure
simple operations procedure that can be controlled from the ground (loaded, edited, started, stopped, etc.) or can be invoked by the occurrence of a predefined on-board event

NOTE In its simplest implementation, an operations procedure can consist of a sequence of low-level commands, historically referred to as a macrocommand.

3.2.17
parameter
elementary data item on-board

NOTE A parameter has a unique interpretation.

3.2.18
parameter validity
conditions that determine whether the interpretation of a given telemetry parameter is meaningful

EXAMPLE The angular output of a gyro may only have a valid engineering meaning if the power to the gyro is “on” while at other times, the output may be random, or at best should not be relied upon.

NOTE Such a parameter is deemed conditionally valid, with its validity determined from the power status.

3.2.19
protection system
on-board function (implemented either in hardware or software) that is provided to monitor sensor or logic readings and, based on their output, either direct or processed, to:

— prevent the propagation of the failure at equipment or system level; or

—

3.2.25
telecommand criticality

importance of a telecommand in terms of the nature and significance of its on-board effect

NOTE Telecommand criticality levels are categorized as Levels A to D as defined in 3.2.25.1 to 3.2.25.4.

3.2.25.1
Level A

5 Autonomy levels

Tables 1 and 2 identify a number of autonomy levels for routine and contingency operations in terms of the corresponding on-board autonomous capabilities.

It should be noted that different autonomy levels may be implemented for routine and contingency operations (i.e. the implementation of Level *n* for routine operations does not necessarily imply the implementation of the same Level *n*

Table 2 — Autonomy levels for contingency operations

Level	Description
C1	Survival mode switching in the event of failures that can be critical for survival (e.g. a power supply short circuit or loss of attitude). No automatic attempt to continue mission product generation.
C2	Redundancy switching for vital functions with the objective of continuing mission product generation (problem analysis and reconfiguration back to prime chain performed under ground control).
C3	Fully autonomous fault management

6 General requirements

6.1 Observability

OBSERV-0010 The space segment shall provide visibility of its internal status and configuration to the mission control system in sufficient detail and within time delays consistent with nominal and non-nominal operations.

6.2 Commandability

CMD-0010 Control functions (telecommands) shall be provided at each level of the design hierarchy to enable mission objectives to be achieved under all foreseeable circumstances (including the use of redundant equipment where required to meet the overall system reliability requirements).

6.3 Compatibility

COMPAT-0020 The space segment design shall be compatible with the availability and capacity of the space-to-Earth communication links for both routine and contingency operations.

6.4 Security

SECUR-0010 The space segment shall be adequately protected against intentional or unintentional access by unauthorized parties.

6.5 Safety

The safety activities related to the following safety requirements shall be performed in accordance with ISO 14620-1.

SAFETY-0010 No single command shall lead to the loss of the space segment.

SAFETY-0030 No single operational error shall result in a failure, and no single failure shall result in another failure. Exceptions to this requirement shall be identified, part of contractual requirements, dealt with in accordance with the safety programme defined in ISO 14620-1, and, where possible, operational contingency procedures shall be defined to mitigate the results of such failures.

SAFETY-0040 The design of the space segment shall be such that all foreseeable on-board failure potentially leading to the loss of the space segment can be averted either by autonomous on-board action when outside ground contact or by clear, unambiguous and timely notification of the problem to the ground. In the latter case, a well-defined recovery procedure shall exist.

SAFETY-0050 It shall be ensured that any reconfiguration of the spacecraft (required for offline testing or any other purpose) shall be such that no single failure either in a control function or in any other element leads to a hazardous on-board situation.

6.6 Flexibility

FLEX-0010 The on-board systems shall be configurable to comply with the desired controllability.

FLEX-0020 The spacecraft shall have the capability to operate with the prime and redundant equipment with the same operability characteristics.

FLEX-0030 The spacecraft shall be configurable such that permanent work-around solutions can be introduced in the event of non-recoverable failure.

FLEX-0050 Any selection and operation of redundant equipment shall be reversible without loss of functionality.

FLEX-0050.1 Constraints or monitoring of redundant equipment shall be clearly identified.

FLEX-0060 In case of contingency operations, inputs and outputs of the on-board functions shall be accessible from the ground for workarounds.

FLEX-0060.1 It shall be possible to replace on-board functions by ground functions.

FLEX-0070

TEST-0020 An “are you alive” function shall be provided for testing the end-to-end connection between the ground and an application process.

TEST-0030 It shall be possible to check redundant on-board functions in an “off-line” manner (i.e. in parallel with the prime function, but without any disturbance to it).

TEST-0040 Adequate observability and commandability shall be provided to assess the proper functioning at the redundant cross-strapped level.

TEST-0050 It shall be possible to check a redundant unit prior to switchover.

TEST-0060 It shall be possible to load and check redundant memory prior to switchover.

TEST-0070

l) the separation status of any separated or deployed piece of equipment.

This data shall be telemetred to the ground in a complete, unambiguous and timely manner.

Where these goals cannot be met, other observables shall be identified to determine the status of the listed parameters.

TMDES-1020 The current state of the spacecraft and any anomalous condition that requires ground intervention shall be available in a sub-set of data.

TMDES-1020.1 An appropriate reserved bandwidth shall be provided for this data (even though it may not always be used).

TMDES-1030 Parameters that indicate vital spacecraft health functions shall be provided with redundant telemetry (e.g. primary bus current, voltage, propellant tank pressure, etc.).

TMDES-1040 Telemetry information shall be provided from direct measurements rather than secondary effects. In particular, the complete status of the spacecraft shall be derivable from the telemetry and other observables without the need for reference to the telecommand history or any record of on-board autonomous actions.

TMDES-1050 In some cases, parameters can change value for very short time periods. If it is necessary, for operational reasons, to detect such occurrences (e.g. as an indication of an on-board failure) and no adequate telemetry sampling of the parameter can be provided, the event shall be stored and the stored value shall be telemetred.

TMDES-1060 For equipment in hot redundancy, telemetry shall be implemented to allow an independent and unambiguous status evaluation of each chain. For elements in redundancy, the loss or failure of one channel shall not prevent access to the telemetry of the other channel.

TMDES-1070 Parameters valid only when other conditions are satisfied shall be determinable unambiguously from the telemetry.

TMDES-1080 Processors/memory auto-test results and diagnoses shall be available through telemetry.

TMDES-1090 The value of analogue parameters shall be derivable from telemetry such that the resolution and range is appropriate for monitoring purposes in all nominal and foreseen contingency situations.

TMDES-1100 Suitable sampling sequences and frequencies shall be provided for all related parameters that require direct correlation or combination for the purposes of performance evaluation.

TMDES-1110 All reconfigurations shall end with an unambiguously known and observable state of all involved units and software.

TMDES-1120 Telemetry shall be provided to isolate any identified failure at least down to function or equipment level.

7.1.2 Telemetry timing information

TIMING-1010 For different operational purposes (e.g. detailed performance evaluation, data or event correlation at the time of on-board anomalies, etc.) it shall be possible via analysis to establish the original on-board sampling time of the telemetry parameters.

TIMING-1010.1 For anomaly troubleshooting, it shall be possible to establish this information retroactively in time.

TIMING-1010.2 It shall be possible to determine the absolute (on-board) sampling time of parameters to an accuracy of <PARAM_ABS_SAMPL_TIME> (can be parameter-specific).

TIMING-1010.3 It shall be possible to determine the relative sampling time of any two parameters to an accuracy of <PARAM_REL_SAMPL_TIME>.

TIMING-1020 Timing information shall be provided in the telemetry that allows the correlation of on-board time with ground time with an accuracy of <TIME_CORREL_ACCUR>.

TIMING-1030 All timing information in the telemetry shall be synchronized with a single on-board master

c) the loading/updating of all monitoring and reconfiguration criteria;

d) the loading/dumping of re-programmable memory areas.

TCDES-1080 It shall be possible to command all on-board devices individually from the ground (i.e. if a device is normally commanded using a telecommand function generated by on-board process, it shall nevertheless be possible for the ground to issue a device telecommand destined solely for that device).

TCDES-1100 The operation of reconfiguring on-board units or switching between on-board functions shall not affect the status, configuration, or continued proper operation of any other unit or function.

TCDES-1110 Where necessary to meet critical mission requirement, it shall be possible to pre-configure units in the “off” state to come on in any desired configuration.

EXAMPLE The bolometer inhibition status of an infrared attitude sensor.

TCDES-1120 There shall be no requirement for the ground to send telecommands, as the result of anomalies detected from the telemetry, with a response time of less than <ANOM_RESP_TIME> (typically 1 min).

TCDES-1130 The level or value of an on-board register or counter shall only be adjusted (from the ground) by the use of a register load telecommand (i.e. on/off pulses shall not be used).

TCDES-1140 For in-orbit operation, the conditions under which a configuration-dependent telecommand may be sent (or may not be sent) shall be determinable unambiguously from the telemetry indicating the status of the spacecraft.

7.2.2 Critical telecommands

The definition of telecommand criticality levels is given in 3.2.25.

CRITTC-1010 Telecommands of criticality Level A or Level B shall require at least two separate command actions for execution, i.e. an arm/safe or enable/disable command followed by an execute command.

EXAMPLE Commands for pyrotechnic devices.

CRITTC-1020 Redundant telecommands shall be provided for all telecommands of criticality Levels A and B by means of a maximum diversity on-board routing (i.e. using on-board routes that share no common nodes or paths).

CRITTC-1030 A register load telecommand of criticality Level A, B or C shall have a separate execute command to permit verification of the loaded data.

CRITTC-1040 For commands of criticality Level A or Level B, on-board protection shall be implemented to ensure that commands are only accepted if the on-board context is correct.

CRITTC-1050 Forbidden telecommands (criticality Level A) shall either be omitted from the spacecraft databases or shall be clearly identified to allow proper ground system processing.

7.2.3 Control of autonomous functions

CONTR-1010 The spacecraft shall provide the capability to enable/inhibit/command any of its on-board autonomous functions.

CONTR-1020 The ground shall have the capability to override any on-board automatic functions.

CONTR-1030 For all on-board automatic functions resulting from a logical combination of several elementary monitoring criteria, inhibition and authorization shall be possible independently and individually for each criterion.

7.2.4 Telecommand transmission and distribution

TCTRANS-1010 The on-board reception, processing, and distribution of telecommands shall ensure that no restrictions arise when the ground transmits telecommands of any type at the highest possible rate (i.e. making full use of the available uplink bandwidth), unless the ground system has specific features to allow adaptable command spacing.

TCTRANS-1020 In order to circumvent potential lock-out problems affecting telecommand routing and delivery, it shall be possible to route a limited number of selected device telecommands directly to the end-item device (i.e. without the need for any intervening software or on-board bus).

7.2.5 Telecommand verification

TCVERIF-1010 Verification telemetry shall be provided for all telecommands that have been properly executed, whether these are sent directly from the ground, are stored on-board for release at a later time, or are generated autonomously on-board.

TCVERIF-1020 Verification telemetry shall be provided with a delay of less than <TC_VERIF_DELAY> with respect to the time of completion of the telecommand execution (typically less than 1 min).

TCVERIF-1030 A telecommand shall be verified by telemetry measured directly for the device or function for which the telecommand is executed (e.g. a device telecommand shall be verified by a hardware measurement that is directly telemetred without intermediate processing).

TCVERIF-1040 If a telecommand results directly in one or more changes in the spacecraft configuration, these changes shall be reflected in the telemetry indicating the spacecraft status.

TCVERIF-1050 Multidata commands (e.g. register load commands) controlling subsystem equipment configurations shall be acknowledged by telemetring all data (e.g. the corresponding register contents).

TCVERIF-1060 The ground shall be notified of any telecommand not executed, not received properly, or not executed properly.

7.3 Memory management

MMGMT-1010 Integrity of the memory area during the load/dump/check process shall be ensured by on-board application processes or by procedural inhibits/constraints. Memory integrity typically requires that no other application process shall have read/write access to this memory area during the load/check process. It is recommended that on-board processes ensure the integrity of memory since this provides a significantly more robust data load operation. Procedural inhibits/constraints should be minimized.

MMGMT-1020 It shall be possible for the ground to load/dump/check any changeable on-board memory area [e.g. random access memory (RAM) or electrically erasable programmable read only memory (EEPROM)].

EXAMPLE R.

MMGMT-1030 It shall be possible either to load, with a single telecommand message, a contiguous memory area (e.g. indicating the start address and the length of the load) or to perform scatter loads (e.g. specifying pairs of memory addresses and data to be loaded).

MMGMT-1040 It shall be possible either to request a memory dump, with a single telecommand sequence, from a contiguous memory area (e.g. indicating the start address and the length of the dump) or to perform scatter dumps (e.g. specifying pairs of memory addresses and length to be dumped).

MMGMT-1050 It shall be possible either to request a memory check, with a single telecommand, from a contiguous memory area (e.g. specifying the start address and the length of the area to be checked) or to perform checks on several areas (e.g. specifying pairs of memory addresses and length to be checked).

MMGMT-1060 Address data loading shall always be performed in the same order.

EXAMPLE Most significant word (MSW) loaded before least significant word.

MMGMT-1070 Where possible, critical on-board storage/buffer should be resizable to cater to unforeseen mission events.

7.4 On-board processing functions

7.4.1 Control loops

CLOOP-1010 The design of the overall mission operations system (i.e. constituting both the ground and space segments) shall ensure that control loops that have short response times are implemented on-board.

CLOOP-1020

OBMON-1050 When on-board monitoring of a specific parameter is mode-dependent, then this shall be defined and automatically selected on-board.

7.4.3 On-board operations scheduling

OBSCH-1010^{R2} It shall be possible to release any telecommand from the on-board operations schedule.

OBSCH-1020^{R2} The status of the on-board operations schedule shall be periodically telemetred to the ground.

OBSCH-1030^{R2} It shall be possible to start/stop the on-board operations schedule.

OBSCH-1040^{R2} It shall be possible to load/add/delete any part of, or any command in, the on-board operations schedule.

OBSCH-1050^{R2}

monitoring and control purposes, for a duration at least equal to the longest non-coverage period plus a mission-dependent margin <DATA_STORAGE_TIME>, typically one orbit for low-Earth orbiting spacecraft.

STORE-1050[R3] On-board storage shall be such that the ground can retrieve the stored data within specified delays <DATA_RETR_DELAY>. There may be several such parameters for a given mission, corresponding to data of different parts of the mission.

EXAMPLE Data such as anomaly telemetry, are normally needed on the ground with shorter delays than routine status telemetry.

7.4.6 Mission management

MIMGT-1010[R2] The design of the on-board mission management function and the associated autonomy duration <AUT_DUR> shall take into account mission-specific factors such as

a) mission product availability requirements;

b) space segment and ground segment complexity;

c) ground station coverage;

d) communications outages due to orbital events (e.g. solar conjunction periods);

e) ground segment non-availability.

MIMGT-1020[R2] During the autonomy duration period <AUT_DUR>, when no action is possible from the ground, the mission management function shall:

- without spacecraft failure, be capable of performing all needed actions to maintain mission operations;

- with spacecraft failure, be capable of avoiding the loss of the spacecraft.

MIMGT-1030[R2] The mission management function shall be hierarchically structured and accommodated as a distributed system in the various processors available on-board. The guiding principle for the distribution of functions is that control shall be exercised at the lowest possible level.

MIMGT-1040[R2] The management of subsystem and payload internal commanding, including all necessary relative time control, shall reside in the corresponding subsystem and payload application processes. This may be in the form of:

- software control processes, using look-up tables if necessary;

- on-board operations procedures.

MIMGT-1050[R2] For the attitude and orbit acquisition phase, it shall be possible to initiate or reconfigure the sequence of operations used in this phase:

a) in an autonomous way, with a possibility of handover from the ground;

b) directly and manually from the ground, if necessary.

MIMGT-1050.1[R2] An automatic sequence shall be initiated on-board upon detection of launcher separation to obtain a safe configuration without ground intervention.

MIMGT-1050.2[R2] It shall be possible to tune on-board delays to follow critical operations from selected ground stations.

EXAMPLE Some pyrotechnic sequences, appendage deployments or first manoeuvres.

7.4.7 On-board fault management

The primary purpose of on-board monitoring is to reduce the necessity for continuously transmitting all the low-level housekeeping data to the ground or for the ground to be continuously available to monitor these data.

FAULT-1010 The design of the on-board fault management function and the associated autonomy duration <AUT_DUR> shall take into account mission-specific factors such as:

a) mission product availability requirements;

b) space segment and ground segment complexity;

c) fault tolerance;

d) ground station coverage;

e) communications outages due to orbital events (e.g. solar conjunction periods);

f) ground segment non-availability.

FAULT-1020 The on-board fault management function shall be capable of performing all necessary actions to react to on-board faults during the autonomy duration <AUT_DUR> without any actions from the ground.

FAULT-1030^{C3} The management of anomalies and failures within a subsystem or payload shall be accommodated within their own application processes. This implies that within each of these application processes, functions shall be provided to detect all internal failures that either endanger the subsystem or payload in question or would lead to severe degradation of mission products. These functions shall also be able to execute internal failure correction actions.

FAULT-1040 Failure detection algorithms shall not repeat the generation of the same exception telemetry if the same failure is detected at each successive failure detection cycle, although a separate telemetry indication should be generated if the exception condition disappears.

FAULT-1050 The fault detection functions shall run independently from the functions being monitored and should wherever possible be based on independent inputs.

FAULT-1060^{C3} It shall be possible to detect faults in systems that are off-line (i.e. not involved in any primary function) as well as on-line.

FAULT-1070^{C1}

FAULT-1100^{C3} The mission manager shall be able to detect system-level anomalies that cannot be recognized by subsystems or payloads.

FAULT-1110^{C3} The mission manager shall handle the management of both system-level anomalies and system-level reactions to subsystem or payload internal anomalies. This implies that the mission manager shall be able to determine whether an internal failure within a subsystem or payload necessitates reconfiguration of other subsystems. If so, it shall determine which reconfiguration steps or procedures shall be applied and issue the corresponding commands to the subsystems or payloads.

FAULT-1120^{C3}

PRSO-1020 If an on-board processor is switched from a prime to a redundant unit (or vice versa), the switchover shall be seamless. This implies that it shall either not be necessary to re-load the operational context from ground (autonomy level R5/C3) or it shall be possible to load the new processor before the switchover.

PRSO-1020.1 R5/C3 The switchover shall not invalidate on-board commands or operation schedules that are already defined for future operations (this implies that the commands defined for the prime unit shall also be valid when loaded in the redundant unit).

PRSO-1020.2 The switchover shall not invalidate any commands in a ground schedule that are already defined for future operations (this implies that the commands defined for the prime unit shall also be valid for the redundant unit, except for the command routing bits which the ground system can automatically change when addressing the redundant processor).

PRSO-1030 A redundant processor shall provide the capability to be turned on and operated out of the control loop, for the purpose of evaluating its performance prior to switching to it as the prime controller.

PRSO-1040

7.5.2 Power supply and consumption

POWER-1010 The power for telemetry conditioning of equipment shall be hierarchically structured and, in particular, shall not be supplied from other unrelated units that are not permanently powered.

POWER-1020 There shall be sufficient telemetry parameters assigned that the power available and power demand can be directly established from the telemetry alone. (This becomes critical in eclipse seasons, for instance, when the solar array degrades to a level approaching the sunlit demand plus recharge demand or when the in-eclipse loads closely match the battery capabilities.)

POWER-1030 Adequate means and telemetry shall be provided for the ground to determine the state of charge of each battery throughout all mission phases, to an accuracy of better than 10 %.

POWER-1040 Monitoring of power-dissipating equipment (e.g. converters) shall be performed through the parameters listed by priority order: primary current, temperature and secondary voltage.

POWER-1050 For all units that have a primary consumption greater than <POW_CONS_THRESH>, to be defined on a mission basis, a thermistor on a hot point or a primary current sensor shall be provided and made available through telemetry.

7.5.3 Telemetry, tracking and command (TT&C)

TT&C-1010 Independent access must be maintained using either payload or platform radio frequency (RF) receiver links, to obviate the need to rely on the ground to reinstate the mission support. This implies that the appropriate receivers shall be continuously active.

TT&C-1020

Annex A
(informative)

Mission constants

The mission constants identified within the body of this International Standard are summarized in this annex for informative purposes.

<ANOM_RESP_TIME> The minimum response time for the ground to react to anomalies detected from the telemetry with the generation of a telecommand.

This is applicable for short, well-defined intervals during critical mission phases and for pre-agreed contingencies and anomaly conditions.

<AUT_DUR> The period of time for which the spacecraft can operate autonomously.

A different autonomy duration may apply for routine and contingency operations.

<DATA_RETR_DELAY> The maximum allowable time delay for the ground to retrieve data generated at an earlier time and stored on-board.

There may be several such mission parameters relating to data of different operational priority.

<DATA_STORAGE_TIME> The time for which telemetry data shall be stored on-board for later dumping to ground, over and above the longest time interval without ground coverage.

This is applicable for missions with discontinuous ground coverage.

<GRND_RESP_TIME> The response time for control loops involving the ground.

There may be several such parameters for a given mission.

<MIN_SAMPLE_INT> The minimum time interval down to which it is possible to sample an on-board parameter for telemetring to ground for investigation purposes.

<MIN_SURV_DUR> The minimum time duration for which the survival of the spacecraft shall be ensured (without ground intervention), having entered survival mode following the occurrence of an on-board failure.

<PARAM_ABS_SAMPL_TIME> The accuracy with which it shall be possible to determine the absolute (on-board) sampling time of a telemetry parameter.

<PARAM_REL_SAMPL_TIME> The accuracy with which it shall be possible to determine the relative sampling time of any two telemetry parameters.

<POW_CONS_THRESH> The threshold of electrical power consumption beyond which specific requirements are imposed for the provision of telemetry data.

<RESOURCE_MARGIN> The margin of resources for on-board subsystems and payloads that is available during the mission.

EXAMPLE Power, on-board memory, CPU load, bus traffic or registers.

<TC_VERIF_DELAY> The maximum delay between the execution of a telecommand and its verification within the telemetry.

<TIME_CORREL_ACCUR> The accuracy with which on-board time shall be correlated with ground time.

ICS 49.140

Price based on 24 pages